Published and Copyright (c) 1999 - 2010
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1243 10/22/10

~ EU Kids Not Safe-Savvy ~ People Are Talking! ~ Sites To Be Liable?
~ Oz Court Order via Web ~ Parents Do Monitor Kids ~ Get A Red Wii, More!
~ Sex.com Sells for $13M ~ The Cyberbully Bugaboo! ~ The New MacBook Air!

~ Court to Google: Tell! ~ Most Kids Cyber-Bullied ~ HP Unveils Slate!

-* E-crime More Common Than Real *-
-* Passwords: You're Doing It All Wrong *-
-* US Studying Australian Web Security Program *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Fall is definitely in the air, and a little winter too! The leaves are finally starting to turn in my neck of the woods. We always seem to be "later" than most, but I think that's more to the fact that oak trees tend to turn color than most other tree types. And we seem to have a preponderance of oak trees around here! And, the temps have been dropping drastically the past few days; we even had a quick burst of rain-snow mix early this morning! Pretty soon I'll be kept busy trying to keep up with all of the downed leaves. Another prelude to winter...

Finally had what I hope to be the last of my "frequent-flier" doctor appointments, today. I had a 3-month follow-up with my cardiologist. Had an EKG which was fine, but my blood pressure seems to have climbed since last month. Not as bad a six months ago, but enough to have the doc increase my medication dosage. Unless something changes for the worse, I'm moved to annual check-ups with my primary and specialty doctors. And, I seem to feel okay overall - a good thing.

Lots of interesting news bits for you this week. More on some various "cyber-bullying" topics - some interesting reading. More on cyber security measures here in the U.S., and that ongoing battle. Imagine yourself being Amazon.com, and opening up a $200-plus million tax bill! See what that's all about, and how it could potentially affect us in the future - a seemingly never-ending revenue topic! So, let's move along to these and other news bits for the week!

Until next time...

=~=~=~=

PEOPLE ARE TALKING
compiled by Joe Mirando
joe@atarinews.org

Hidi ho friends and neighbors. It's going to be a short column this week. Lots of things to do and messes to clean up. Another week has come and gone and, depending on where you live, the leaves are in the process of

changing. The things that trees do in the autumn have always amazed me. What a wonder feat of engineering they are, not only for their rich deep colors, but for the fact that they exist at all.

Now I’m not going to go into a tirade and spout a bunch of Intelligent Design nonsense, but it DOES amaze me that there is such wondrous complexity... and to show my ’human arrogance’... that it all took place without us doing anything.

I mean, look at how a tree works. It grows in the ground, extracting nutrients from nothing but the earth, using sunlight and rain water and the dirt and nothing else.

Think about it; A tree is a kind of.. chemical processing ’plant’. It takes nitrogen and other various chemicals, along with water, from the ground, uses chemical processes powered by sunlight and produces living matter. It grows. It does not ’build’, but creates.

And when it’s this time of year, the trees shut down. The leaves undergo changes and fall off. But they’re not wasted. Trees know... the leaves, mixed with anaerobic bacteria, will decompose and return nutrients to the soil, enriching it for the spring. The tree slows down and settles in for the coming winter, preparing for what’s to come.

All winter long it survives by doing as little as it can, storing its growth to nothing, protecting itself against the cold, getting ready to start it all over in the spring.

When spring comes, it activates again, pulling water and nutrients from the ground, sprouting leaves to catch the sun, putting out new shoots and stems. Sap starts running again, without the benefit of a heart to pump. Branches turn toward the sun, without the benefit of muscles. It puts out fruits or seeds to ensure the continuation of its species, all without a brain to tell it what to do or when.

Yes, it amazes me that what we take for granted because we see it every day is really so special. It’s a wonder. Have you ever stopped to wonder how wood is ’made’? Think about it; that stuff has to come from somewhere, and I don’t know if any of US could craft something like a tree from nothing but dirt and water and sunlight. And not only ’craft something’, but something that grows and can reproduce.

Oh, and by the way, in addition to growing on its own, it and its green brethren make OUR lives possible in large part. I did make one mistake above. In addition to water and ’dirt’ and sunlight, there is one thing that trees also need. Carbon dioxide. They take in carbon dioxide (without the benefit of lungs, I might add) and break it down. The carbon gets used in making wood, and the oxygen gets released into the air.. for us to breathe.

It’s true that most of the oxygen in our atmosphere comes from the algae in the oceans, but some of it comes from large areas of foliage like the Amazon basin, and forests. And every single tree does it. Every tree you pass on the road is taking in carbon dioxide and putting out oxygen.

So the next time you "knock on wood" or lean against a fencepost or sit under an apple tree to try to discover a law of nature or something, think about the tree too.

Of course, what led ME to think about this is that I’ve got a lot of

raking to do... all those ’solar collectors’ are hitting the ground now.

Well, that’s it for this time around. Tune in again next week, same time, same station, and be ready to listen to what they are saying when...

PEOPLE ARE TALKING

=~=~=~=

->In This Week’s Gaming Section - Nintendo Releases Red Wii, and more!
  """""""""""""""""""""""""""""""""

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
  """""""""""""""""""""""""""""""""""""""

Nintendo Releases Red Wii, DSi XL Bundles, Wii Remote Plus

In celebration of the 25th anniversary of the Super Mario Bros. game, Nintendo on Thursday released red Wii and DSi XL bundles, as well as the new Wii Remote Plus.

The limited-edition lineup will be available in North America on Nov. 7.

First up is a red Wii bundle, which includes a red Wii console, the "Super Mario Bros." Wii game, a new red Wii Remote Plus controller, Wii sports, and a red Nunchuck controller. It will sell for $199.99, and is available for pre-order
now.

The red Nintendo DSi XL bundle, meanwhile, includes a red DSi XL with special artwork, the "Mario Kart" DS video game, three pre-installed titles and built-in software, including "Brain Age Express: Arts & Letters" and "Brain Age Express: Math and Photo Clock." The bundle also add a large, red stylus. It will sell for $179.99 and is also available for pre-order.

Nintendo also announced the Wii Remote Plus, which adds Wii MotionPlus functionality. It will become the standard Wii controller going forward and will be included in upcoming Wii hardware packages and bundles. It will be sold separately for $39.99, or bundled with the new FlingSmash motion control game for $49.99.

"Whether shoppers want to add a cool new look to their gaming setup or expand their supply of controllers with an exciting game, Nintendo offers

a great value for the holidays," Marc Franklin, Nintendo of America's director of public relations, said in a statement. "For anyone who is still on the fence about whether to join the world of video games, we're offering many fun, easy, economical ways to get involved."

Earlier this week, Netflix announced that Wii users will no longer need a disc to stream its Watch Instantly content from the console. The next big launch for Nintendo is expected to be its 3DS, which should launch in the U.S. in March for $300.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

E-crime Now More Common Than Real Crime

If there was any doubt about the popularity of electronic dupery, it should be put to rest with a report on global fraud released the week by the risk management consulting firm Kroll. For the first time since 2007, when the company began putting together its annual survey on crime, electronic fraud surpassed physical scams as the most common form of fraud in the world.

In the past theft of physical assets or stock topped the report's fraud charts, but this year's survey--performed by the Economist's Intelligence Unit and based on information gathered from more than 800 senior executives worldwide - showed information theft, loss or attack edging out physical fraud by a razor thin margin of 27.3 to 27.2 percent.

While that margin may be small, the year-to-year increase for information fraud isn't. Last year, information theft finished third in the fraud rankings with 18 percent of the companies in the survey reporting info scams, compared to 28 percent reporting physical fraud and 20 percent management conflict of interest frauds.

The growing trend in information fraud isn't about to abate, either, the report said. "The survey suggests that things may get worse before they get better," it noted. "Information theft or attack is the type of fraud to which respondents are most likely to describe their companies as vulnerable (37 percent)."

"Again," it continued, "their concerns are not isolated. This type of crime is regarded as the greatest weak spot for three of the 10 industries covered in the survey - Financial Services, Professional Services, and Natural Resources and the second greatest for three more - Construction, Technology, Media and Telecoms, and Retail."

Although corruption topped the list cited by companies for avoiding expanding into foreign countries (17 percent) or investing in them (37 percent), information theft came in second, with nine percent of respondents refusing to do business in some regions because of it and 19 percent eschewing investment for fear of it.

"In most geographies information theft is the second biggest deterrent to investment, but that varies widely, from seven percent in Western Europe to 31 percent in neighboring Central and Eastern Europe," the report said.

US Studying Australian Internet Security Program

The government is reviewing an Australian program that will allow Internet service providers to alert customers if their computers are taken over by hackers and could limit online access if people don't fix the problem.

Obama administration officials have met with industry leaders and experts to find ways to increase online safety while trying to balance securing the Internet and guarding people's privacy and civil liberties.

Experts and U.S. officials are interested in portions of the plan, set to go into effect in Australia in December. But any move toward Internet regulation or monitoring by the U.S. government or industry could trigger fierce opposition from the public.

The discussions come as private, corporate and government computers across the U.S. are increasingly being taken over and exploited by hackers and other computer criminals.

White House cybercoordinator Howard Schmidt told The Associated Press that the U.S. is looking at a number of voluntary ways to help the public and small businesses better protect themselves online.

Possibilities include provisions in the Australia plan that enable customers to get warnings from their Internet providers if their computer gets taken over by hackers through a botnet.

A botnet is a network of infected computers that can number in the thousands and that network is usually controlled by hackers through a small number of scattered PCs. Computer owners are often unaware that their machine is linked to a botnet and is being used to shut down targeted websites, distribute malicious code or spread spam.

If a company is willing to give its customers better online security, the American public will go along with that, Schmidt said.

"Without security you have no privacy. And many of us that care deeply about our privacy look to make sure our systems are secure," Schmidt said in an interview. Internet service providers, he added, can help "make sure our systems are cleaned up if they're infected and keep them clean."

But officials are stopping short of advocating an option in the Australian plan that allows Internet providers to wall off or limit online usage by customers who fail to clean their infected computers, saying this would be technically difficult and likely run into opposition.

"In my view, the United States is probably going to be well behind other nations in stepping into a lot of these new areas," said Prescott Winter, former chief technology officer for the National Security Agency, who is now at the California-based cybersecurity firm, ArcSight.

In the U.S., he said, the Internet is viewed as a technological wild west

that should remain unfenced and unfettered. But he said this open range isn’t secure, so "we need to take steps to make it safe, reliable and resilient."

"I think that, quite frankly, there will be other governments who will finally say, at least for their parts of the Internet, as the Australians have apparently done, we think we can do better."

Cybersecurity expert James Lewis, a senior fellow at the Center for Strategic and International Studies, said that Internet providers are nervous about any increase in regulations, and they worry about consumer reaction to monitoring or other security controls.

Online customers, he said, may not want their service provider to cut off their Internet access if their computer is infected. And they may balk at being forced to keep their computers free of botnets or infections.

But they may be amenable to having their Internet provider warn them of cyberattacks and help them clear the malicious software off their computers by providing instructions, patches or anti-virus programs.

They may even be willing to pay a small price each month for the service - much like telephone customers used to pay a minimal monthly charge to cover repairs.

Lewis, who has been studying the issue for CSIS, said it is inevitable that one day carriers will play a role in defending online customers from computer attack.

Comcast Corp. is expanding a Denver pilot program that alerts customers whose computers are controlled through a botnet. The carrier provides free antivirus software and other assistance to clean the malware off the machine, said Cathy Avgiris, senior vice president at Comcast.

The program does not require customers to fix their computers or limit the online usage of people who refuse to do the repairs.

Avgiris said that the program will roll out across the country over the next three months. "We don’t want to panic customers. We want to make sure they are comfortable. Beyond that, I hope that we pave the way for others to take these steps."

Voluntary programs will not be enough, said Dale Meyerrose, vice president and general manager of Cyber Integrated Solutions at Harris Corporation.

"There are people starting to make the point that we’ve gone about as far as we can with voluntary kinds of things, we need to have things that have more teeth in them, like standards," said Meyerrose.

For example, he said, coffee shops or airports might limit their wireless services to laptops equipped with certain protective technology. Internet providers might qualify for specific tax benefits if they put programs in place, he said.

Unfortunately, he said, it may take a serious attack before the government or industry impose such standards and programs.

In Australia, Internet providers will be able to take a range of actions to limit the damage from infected computers, from issuing warnings to restricting outbound e-mail. They could also temporarily quarantine

compromised machines while providing customers with links to help fix the problem.

Half of EU Kids Don’t Know How to Be Safe Online

Half of the young children in the E.U. don’t have basic Internet safety skills such as knowing how to control privacy settings or block unwanted contacts.

However, the threats faced by children online are steadily decreasing, according to a new study by the European Commission. Only 5 percent of children in Europe say that they have been bullied online, with a high of 14 percent in Estonia and Romania.

The EUKidsOnline survey interviewed more than 23,000 children and one of their parents in 22 E.U. member states, as well as Turkey and Norway. It found that, on average, European children start using the Internet at the age of seven, but a third of children between the ages of nine and 12 feel that there are enough "good things for kids" online.

Broadly speaking, children go online the earliest in the Nordic countries, the Netherlands and U.K., and later in Mediterranean countries. The most active young Internet users are aged 15 and 16, with 77 percent going online daily.

Children in the survey say they use the Internet primarily for school work or watching videos (84 percent and 83 percent respectively), playing games (74 percent) and communicating via instant message (61 percent).

The vast majority of children use the Internet at home (85 percent), with school in second place (63 percent). Although children mainly use computers to go online, the survey found that one-third now connect via mobile devices.

Virus Fighting: An International Sport

Microsoft is an American company, as is Apple. In the antivirus world some of the big names like Norton and McAfee are American, but they’re in the minority. Kaspersky, a huge seller in American retail stores, is based in Russia. The popular Spyware Doctor antivirus/antispyware tool comes from Australia. While they’re all competitors for your attention and shopping dollars, they work together against the forces of software evil. Nowhere is this clearer than in a meeting of Anti-Malware Testing Standards Organization (AMTSO).

Founded in 2008, AMTSO is dedicated to ensuring that testing of anti-malware software is conducted fairly, accurately, and consistently. Yes, the vendors are in competition with each other; so when there’s a published comparison test they want dependable results. To this end AMTSO created a set of basic guidelines for testing. The guidelines are quite sensible. For example, testing should be reasonably open and transparent, testing must be unbiased, and the conclusion of a test must be based on test results. Members can submit a published test to the group’s Review Advisory Board; this board reports on how closely the test adheres to

AMTSO guidelines.

There are currently about three dozen members of AMTSO representing at least two dozen countries (some have significant presence in multiple countries). The most recent addition is HCL Technologies, formerly the security division of CA, and it’s a perfect example. The company itself is based in India, but its representative to the current AMTSO meeting, taking place now in Munich, comes from its Italian division.

In addition to the basic guidelines for testing, AMTSO has published a number of other documents on topics including whole-product dynamic testing, validating malware samples, and creating malware for test purposes (summary: don’t!). Representatives at the current meeting will vote on whether to approve a new set of guidelines for testing false positives - those unfortunate times when antivirus software mistakenly identifies a good program as malicious.

Should Sites Be Held Liable for User Comments?

Britain’s Attorney General has said that website owners should be made legally responsible for comments made by visitors.

According to a report on Out-law.com, Dominic Grieve (pictured) told members of the Criminal Bar Association that the spiralling number of internet news web sites meant it was becoming more and more difficult for courts to ensure that trials were fair, and that juries were not exposed to material that could prejudice a hearing.

"The rise of [the Internet] has been profound in so many aspects of our lives, including the relationship between the Courts and the media," Grieve told the assembled audience of lawyers. "The news is constantly available and updated either on 24-hour television networks, the websites of mainstream news organisations, or unofficial blogs, emails and social networking sites. The amount of material is vast and it can be passed on at lightning speed.

"In my view this does not reduce the importance of the contempt of court laws. It doesn’t remove the need for fair and accurate contemporaneous reports," the Tory MP said.

Turning his attention to comments posted by members of the public, Grieve explained:

"If it is increasingly easy for individuals to act as unofficial journalists and publishers the greater the need for general understanding about why restrictions are sometimes necessary. This extends particularly to those who run websites upon which members of the public place their opinions.

"I understand that there is no clear authority in relation to their legal obligation but there must, I feel, be an argument that they too have to ensure that a trial is not prejudiced by what is posted," said Grieve. "I would be happy to have further discussions with such organisations... with a view to increasing their understanding of those potential risks."

Until now, printers and distributors have been able to argue that they had innocently passed on prejudicial material - a defence that could be used by

web site publishers to disclaim responsibility for prejudicial comments, argues technology lawyer Struan Robertson of legal firm Pinsent Masons.

"Site operators could use the ’innocent distribution’ defence, claiming that they did not know that material was sub judice," says Robertson. "This defence is not available once they have been told about the material, though."

"Online publishers that remove that material quickly would also be able to claim a defence under the E-Commerce Regulations that absolve publishers of responsibility for unlawful material as long as they remove it quickly when told about it," said Robertson.

Grieve’s comments suggest he is considering a change in the law to make site publishers responsible for material posted by users, and come after a string of high-profile cases in which courts held that they were powerless to tackle the publishing of prejudicial material.

Extensive coverage of a paternity case in the High Court last year led to the judge ruling that an extension of reporting restrictions was "futile". In another judgment, a court ruled that reporting restrictions only replied to those people who were aware of them - leaving open the question of whether amateur commentators such as bloggers may be able to evade restrictions that bound more professional news outlets.

43 Percent of Teens Affected by Cyber Bullying

Most kids have been the target of cyber bullying, according to a Wednesday report. A study commissioned by the National Crime Prevention Council found that 43 percent of kids were on the receiving end of this kind of harassment last year.

Of the 824 teens surveyed by the council, 78 percent have been using the Web for at least three years, while 96 percent have an e-mail account. Despite the common presence of teens online, however, many have very little parental supervision.

The study found that 43 percent of teens said that "their parents usually know what they’re doing online, but do not have any rules about their activity" and about 27 percent said their parents have no idea what they’re doing online. About 23 percent have and follow their parents’ rules.

As a result, 43 percent said they have experienced some sort of cyber bullying. The trend was much more common among females, with 51 percent reporting that they’ve experienced the harassment in some form, while 37 percent of men said the same. Cyber bullying is most rampant among high school students, the survey reported.

"While 46 percent of high school teens have experienced cyber bullying, only 35 percent of middle school students have had that experience," it said.

The Harris poll said that cyber bullying is most likely to occur among 15 and 16-year-olds.

This information is especially timely in light of the wave of teen suicides that have taken place as a result of cyber-bullying. Tyler

Clementi was a Rutgers University student who jumped to his death from the George Washington Bridge after his roommate and another student posted footage on the Internet of Clementi's sexual encounter with another man.

In the wake of this and other teen suicides, Facebook recently announced of a partnership between several organizations to curb hate speech on its site. The collaboration includes MTV's a Thin Line campaign, the Gay and Lesbian Alliance Against Defamation (GLAAD), the Human Rights Campaign (HRC), the Trevor Project, the Gay, Lesbian, and Straight Education Network (GLSEN), and Parents, Families & Friends of Lesbians and Gays (PFLAG).

Court to Google: Tell New Yorker Who Posted About Her

A business consultant who wants to know who's been anonymously disparaging and fixating on her online has gotten a court to force Google to tell her.

As she joined a growing number of people who have persuaded courts to unmask troublesome cyber ciphers, Carla Franklin said Wednesday she hoped her case would help others combat similar problems.

"The Internet cannot become a safe haven for harassers and stalkers," she said in an e-mail.

Google Inc. declined to comment. The Mountain View, Calif.-based online giant says it doesn't discuss individual cases to protect users' privacy, but it follows applicable laws.

A Manhattan court ruling issued Tuesday gives the company a couple of weeks to provide Franklin with identity and contact information for the person or people who posted denigrating comments and unauthorized videos of her, beginning last year.

The videos, posted on Google-owned YouTube, were clips from an innocuous student film in which she had appeared years before, coupled with personal information about her to create an unsettling online shrine, she said. Franklin did some modeling and acting before becoming a consultant to nonprofit organizations.

The comments, made though another YouTube channel, featured a sexual slur and were posted alongside videos she made for Columbia Business School while earning a master's degree there, she said.

The postings were humiliating, creepy and potentially hurtful to Franklin's professional prospects, she and her lawyer have said.

Franklin said in a blog post of her own this month that she believes she knows who's responsible, but she went to court last summer to get proof so she could potentially pursue further legal action. Her court case didn't involve Columbia.

While anonymous commentary became an instant tradition and valued aspect of the Internet, it's also become a scourge for people and businesses who have found themselves bullied and besmirched by shadowy critics. And it's become an issue for courts trying to weigh self-expression rights against defamation and other legal claims.

"There’s a tension there - there’s a First Amendment right to be able to speak anonymously, but there’s no First Amendment right to violate the law," said Bennet G. Kelley, a Santa Monica, Calif., attorney who specializes in Internet law.

"People think: ’It’s the Internet. I can do whatever I want,’" he said, but "the law applies, online and offline."

Still, enforcing it can be a challenge. While a number of states have laws against cyberharassment or cyberstalking, it can be difficult for authorities to go after suspects who can easily change aliases and may be in another jurisdiction.

Prosecutions do happen, including the recent trial of a New York man accused of using phony online identities to harass and discredit his scholar father’s adversaries in a heated academic debate over the origins of the Dead Sea Scrolls.

The son, Raphael Golb, was convicted last month of identity theft and other charges. He said his pseudonymous e-mails and blog posts amounted to academic whistle-blowing and satire, not crime; he plans to appeal.

Some people end up going to court themselves to stop being trashed online. In one high-profile case, Vogue cover model Liskula Cohen successfully sued Google in a New York court last year to get the name of a blogger who had made derogatory remarks about Cohen’s hygiene and sexual habits.

Cohen said the comments on the site were defamatory. The blogger, ultimately identified by court order as Rosemary Port, said her privacy was violated, and she had a right to her opinions.

Australia Police Serve Court Order via Facebook

Australian police served a court order on an allegedcyber bully using the social networking site Facebook, officials said Wednesday, describing it as a national first.

Victoria police got court approval to use the site after attempts to serve the order in person, over the telephone or via the post failed.

The "prolific" Facebook user was accused of, among other things, using the site to harrass, bully and threaten another person, and police said they transcribed all the court documents and sent them to his Facebook inbox.

A video was also made of the order being read "as if the Respondent was being directly spoken to" and sent electronically to him.

"He stated that he understood the seriousness of the orders, having read ... documents served via the social media website and agreed to comply, stating that he would delete his Facebook profile," a police statement said.

"In this instance we were able to deliver justice through the same medium as the crime committed," said leading senior constable Stuart Walton, the officer in charge of the investigation.

"Police will always pursue traditional means to enforce the law and to protect the community, but we won't shy away from innovative methods to achieve positive outcomes either."

In 2008 an Australian lawyer won the right to serve legal documents via Facebook, the same year a Sydney court allowed lawyers to serve rugby player Sonny Bill Williams with a subpoena via SMS text message.

Australia, with a population of 22.5 million, has almost nine million Facebook users.

The Cyberbully Bugaboo

I'm not particularly pleased with the continued use of the concept of the "cyberbully" when talking about what is clearly a situation involving libel or slander.

The case at hand today is that of Carla Franklin. She had a laundry list of complaints, many legitimate, that have been all rolled into the category of cyberbullying by the media and others. The story is all over the news, and the woman is now making TV appearances.

Let's summarize. She felt she was being cyberstalked, which is a concept I never fully understood. You are either stalked or you are not. If someone is dogging you on the Internet, does that constitute cyberstalking? Law enforcement has never even been clear about what action can be taken when you think you're being cyberstalked. Then, she claimed harassment and defamation. This included the posting of a YouTube video someone made of her (the circumstances are not clear) with the word "whore" appearing somehow on the video.

She managed to get a judge to demand the names of the supposed three people involved in the posting of the video and the comments. Two of the names are JOEBOOMO8 and JIMMYJEANOO8, which sounds like the same guy to me.

To track the culprit down, Google will do a little research and pull down the IP addresses which is simple enough. The IP address must then be associated with an ISP. Next, the IP address needs to be linked to a specific subscriber. Then, someone has to prove that the specific subscriber was actually the one using the IP address. If this culprit has an open Wi-Fi account or expert skills, it would be hard to prove he did it. And there is always the remote possibility that the person(s) who did this used a public library, cafe, or stolen Wi-Fi signal. Generally speaking, at this point in the investigation, if zero connection to Ms. Franklin can be shown, everything falls apart and a lot of time was wasted.

In a simple online harassment case like this, the person being harassed either knows the guy on the other end of the line or not.

The person harassing this woman is obviously a co-worker who hates her, a snubbed suitor, an ex-boyfriend, an acquaintance who was wronged, or a random psycho. There are not too many other possibilities. The random psycho is the only dangerous one on the list. If any of the others were dangerous, they would have physically attacked the woman by now, I would think.

That said, something has to be done once in a while to cut down on the online anonymous libel. And I'm not saying this because I'm against people expressing themselves. It just seems as if too few people know what libel is or that it's illegal. A few people need to be ruined (as in prosecuted and jailed) for doing it to put the fear of God into the others. And, yes, you can call someone an a-hole or even a whore, if you do it right. Seriously. But not if it includes a never ending stream of false accusations and harassing commentary.

I suspect this situation will resolve itself once the so-called bully's identity is revealed. I can assure you that will be the most interesting aspect of the story. "Dad! You?!?!" Other than that, this whole incident seems lame and hardly newsworthy.

Most Parents Monitor Kids' Social Networking Regularly

"Oh Crap. My Parents Joined Facebook."

So reads the introduction of an online support group, myparentsjoinedfacebook.com, for the kids of parents who have connected with them online. With rants ranging from a mother who "liked" hundreds of photos on her daughter's page, to another who used Facebook to "out" her son for logging onto Facebook too much, parents may learn a thing or two about how to engage with your teens on social networking sites.

After all, some parents appear to have no shame when it comes to the difference between monitoring and cyber stalking, according to a new study on parent-teen attitudes towards online privacy conducted by San Francisco-based privacy group Truste.

The study showed that 72 percent of the 1,037 parents with social-networking accounts monitored their teen's social-networking accounts regularly, with 35 percent checking every day. Another 10 percent of parents were even secretly logged into their teen's accounts (the survey doesn't share how this was done). Eighteen percent of teens said they have been "disciplined" or "embarrassed" by their parents online.

In fact, although the study said that 84 percent of parents are "confident" that their teen is responsible with posting personal information on a social-networking site, 89 percent wanted these sites to have default privacy settings that limited profile access to their teens' accounts. Another 82 percent wanted the ability to delete their kids' posts; surely an invasion of privacy in itself?

However Truste said its findings were a step in the right direction:

"Our survey shows that parents and teens are engaging together on social networks, that parents actively monitoring teens, and that both teens and parents care about privacy and are using privacy controls (to be fair the teens are probably sometimes using them to hide content from parents)," Truste president Fran Maier wrote in a company blog post.

Maier also admitted to joining Facebook to monitor the online behaviors of her two sons' relationship that has taken some time to foster. Maier's youngest threatened to de-friend her for posting too often on his wall.

Truste also released two sets of privacy recommendations for teens and parents. The first piece of advice for parents: talk, chat and e-mail with your teen about privacy. The first piece of advice for teens: befriend your parents online.

Apple Shows Off iPad-inspired Mac Laptop

Apple Inc CEO Steve Jobs unveiled the thinnest, lightest Mac laptop yet, fusing features from its popular iPhone and iPad with its traditional line of personal computers.

Apple, whose computers have taken market share from PCs based on Microsoft Corp's Windows, will bring a version of its mobile applications store to the Mac, aiming to replicate its success and spur development of new programs.

Loading up Macs with iPad features may help Apple stave off investors' fears that sales will begin bleeding over to the tablet, which has stirred up astonishing demand.

The new MacBook Air - introduced on Wednesday with Jobs' signature "one last thing" set-up - is designed to reproduce the versatility of popular devices such as the iPhone and iPad, and will incorporate FaceTime video chats, which Apple is bringing to all its Macs.

Utilizing flash storage like the iPad rather than hard drives like conventional computers, it can power up almost instantly from standby mode and store data twice as quickly as a standard hard drive. But it sacrifices processing power compared with Apple's other laptops.

"We asked ourselves what would happen if a MacBook and an iPad hooked up? Well, this is the result," Jobs said at a media event in Cupertino, California, calling the Air the "future of notebooks."

It starts at $999 for an 11.6-inch model, weighs as little as 2.3 pounds (1 kg), and measures 0.11 inches at its thinnest to 0.68 inches at the rear.

"They're basically merging the product lines; they're simplifying it," said Kaufman Bros analyst Shaw Wu. "They're taking the strengths out of what they've learned on the iPhone and iPad and bringing that technology over to the Mac side. It makes a lot of sense."

While plenty of attention is lavished on the iPhone and iPad, the Mac has been critical to the company's success over past years. Apple sold $22 billion worth of Macs in fiscal 2010, comprising one-third of its revenue. Shipments rose more than 30 percent and far outpaced the overall market.

Investors have wondered whether the iPad, a 10-inch touchscreen tablet that began selling in April from $499, would cannibalize sales of the Mac - as it has done for low-end, Windows-based laptops known as netbooks.

Gartner analyst Mike McGuire does not expect much cannibalization between iPad and Macs because of the gulf in price tags. He said the Air will try to bridge Apple's newer and older product lines.

"It's that missing link between the tablet future and the existing notebook," he said.

Jobs also showed off a new version of Mac operating software, which the company will release next summer. Nicknamed "Lion," it includes an improved "iLife" multimedia suite and incorporates FaceTime video chat, which the company recently launched on the iPhone.

FaceTime will allow for video calls between iPhones, iPod touches and Macs. Over 19 million Apple devices are already equipped with FaceTime, Jobs said. It released a test version of FaceTime for the Mac on Wednesday.

The App Store for the Mac will go live within 90 days, and developers will be able to start submitting apps next month. They will get 70 percent of the revenue from sales.

The original App Store debuted in 2008 and helped spur sales of the iPhone by providing a wealth of fun, useful or merely diverting programs for sale, at the touch of a button.

It houses more than 250,000 apps and has generated over 7 billion downloads. In addition, more than 30,000 apps have been specifically made for the iPad.

In the third calendar quarter, Apple became the No. 3 personal computer maker in the United States with a 10.6 percent market share, according to IDC. It holds roughly 20 percent of the U.S. consumer market.

But Apple’s global market share is less than 5 percent, and the company is aiming to increase sales outside its U.S. stronghold. The Mac user base overall now stands at nearly 50 million.

HP Unveils $799 Tablet With A PC Feel

Hewlett-Packard Co unveiled its first product for the fast-growing tablet market, a $799 device running Microsoft Windows that is aimed at business customers.

HP’s Slate 500 attempts to replicate the PC experience in a tablet form, providing a contrast to rivals who have brought more of a smartphone feel to their devices. The Slate runs the same version of Windows 7 used by many companies on their standard PCs.

The tablet has a bigger price tag than competing products such as Apple’s iPad, which kick-started the tablet craze when it debuted earlier this year.

HP’s offering has an 8.9-inch, multi-touch-enabled screen, weighs 1.5 pounds and comes with 64 gigabytes (GB) of storage and a digital stylus pen. It gets five hours of battery life.

It comes equipped with Wi-Fi access but no built-in capability to connect to high-speed cellular networks, as rivals including the iPad, Samsung Electronics’ Galaxy Tab and Dell’s Streak have.

Carol Hess-Nickels, director of business notebook marketing at HP, emphasized the Slate’s business utility. She expects retail, healthcare and insurance companies, among others, to build custom applications that take advantage of the device’s portability.

"It’s really like a full-function PC, it runs Windows, it will run your office applications, it just so happens to be in a slate form factor," Hess-Nickels said.

The HP Slate features the Intel Atom processor, which is commonly found in inexpensive netbook computers. Rival tablets run on low-power ARM-based chips found in smartphones.

The device is equipped with cameras in the front and back, enabling video conferencing, and a USB port. It comes with a case and a docking station.

HP’s Slate is now available online, and the company will be selling it to businesses through its direct sales force.

It’s $799 price tag makes it more expensive than the Wi-Fi-only version of the iPad, which starts at $499 and runs up to $699 for a 64-GB model. A 3G iPad starts at $629.

Verizon Wireless plans to sell Samsung’s 7-inch tablet for $600. Dell’s 5-inch Streak is priced at $550 but can be had for $300 if bought with a data plan through AT&T.

HP, the world’s largest PC maker, plans to release a tablet next year that may look much different from the Slate.

That tablet will be based on the webOS software that HP acquired when it bought smartphone maker Palm earlier this year for $1.2 billion. It will likely be a more media-rich and consumer-friendly offering.

The tablet market is expected to surge next year to more than 50 million units, research group Gartner has said. The iPad is expected to continue to be the dominant product in this market.

Apple has sold more than 7 million iPads since the device launched in April.

The market is still evolving, but Apple has targeted the iPad primarily as a consumer device made for media consumption, rather than a business device.

Earlier this month, BlackBerry maker Research in Motion unveiled a 7-inch tablet aimed at business customers.

And Dell has touted the business applications for its tablet, which include healthcare. Dell expects to launch a 7-inch model by the end of the year.

Sex.com and the World’s Most Expensive Domain Names

If there’s one thing we can all agree on, it’s that sex sells.

It should come as no surprise, then, that the Web’s simplest sex-based domain name - sex.com - has just sold for a reported $13 million. Or, to put it in a rhyme, 13 million bucks for a synonym of ... well, you know.

A company from the Caribbean called Clover Holdings is behind the $13

million sex.com bid, according to the BBC. It’s not yet clear what Clover plans to do with the sex.com site (though I think we can all take a guess).

To be sure, 13 million’s no small chunk of change, even in the high-stakes domain game. In fact, if the sex.com sale goes through - it still has to be approved by a court - the name stands to be one of the most expensive in the history of the World Wide InterWebs.

Get this, too: The last sale of sex.com is also among the grandest domain transactions of all time. Back in 2006, original sex.com owner (and Match.com founder) Gary Kremen sold the domain for $12 million. The company that bought it ended up declaring bankruptcy, leading us to where we are today.

So if sex.com is worth $13 million, what other domain names can fetch that kind of cash? According to some records, the current top dollar-grabber is internet.com. A company called QuinStreet reportedly bought the domain for a cool $18 mil back in ’09. QuinStreet is also said to have forked over $16 million for insure.com that same year. Both of those sales, however, appear to have included assets beyond just the names themselves.

The 10 highest priced standalone sales, according to industry magazine Domain Name Journal (as reported by ABC News):

* Fund.com: $9.99 million
* Porn.com: $9.5 million
* Diamonds.com: $7.5 million
* Slots.com: $5.5 million
* Toys.com: $5.1 million
* Vodka.com: $3 million
* Candy.com: $3 million
* CreditCards.com: $2.75 million
* Computers.com: $2.1 million
* Seniors.com: $1.8 million

Man - if we could only find a way to combine a bunch of these into one mega-spectacular super-domain, we’d have a billion dollar idea on our hands.

Wait! I’ve got it: VodkaCandyForSeniorsWhoPlaySlotsOnComputersWithCreditCards.com.

Big money, here I come.

Oracle Wants LibreOffice Members To Leave OOo Council

A group of key OpenOffice.org (OOo) contributors and community members recently decided to fork the project and establish The Document Foundation (TDF) in order to drive forward community-driven development of the open source office suite. Oracle has responded to the move by asking several members of TDF to step down from their positions as representatives on the OOo community council.

During an OOo community council meeting last week, council chair Louis Saurez-Potts told the TDF members who also sit on the OOo community council that their participation in both organizations constituted a conflict of interest and that their involvement in the new LibreOffice

fork should preclude them from holding leadership roles in the OOo community. Saurez-Potts is Oracle's OpenOffice.org community manager, a role that he also held at Sun prior to the acquisition. His position suggests that Oracle views LibreOffice as a hostile fork and will not join TDF as some had hoped.

"Your role in the Document Foundation and LibreOffice makes your role as a representative in the OOo CC untenable and impossible. [I]t causes confusion, it is a plain conflict of interest, as TDF split from OOo," he told TDF members during a council meeting that took place on an IRC channel. "If the TDF members do not disassociate themselves from the [Document Foundation] then they must resign by Tuesday."

OOo council members who also hold leadership roles in TDF include Charles H. Schulz, Christoph Noack, and Cor Nouws. It's unclear how they will proceed now that they have been handed this ultimatum by Oracle.

Texas Sends Amazon.com A $269 Million Tax Bill

Amazon.com Inc said Texas sent it a $269 million bill last month for uncollected sales taxes for purchases that its residents made through the online retailer.

Amazon.com Inc said in a filing on Friday that the state sent the company an assessment in September for uncollected sales taxes from December 2005 to December 2009, including interest and penalties.

Texas claimed Amazon should have collected sales taxes over that period.

"We believe that the State of Texas did not provide a sufficient basis for its assessment and that the assessment is without merit," Amazon said in the filing.

Amazon has found itself under attack over sales tax collection as states deal with their budget deficits. In April, Amazon sued North Carolina's department of revenue, claiming its demand for Amazon to turn over names and buying records of customers violated privacy laws.

Passwords: You're Doing it Wrong

Safe password practices are often the only thing standing between you and identity theft, loss of privacy, and even an empty bank account. Too bad you're not following them. At least, the chances are good that you aren't, according to a survey from security company Webroot.

Webroot surveyed 2,500 people in the U.S., the U.K., and Australia about their password habits, and the results should worry everyone but cybercriminals, who should be delighted. Criminals will also be pleased to hear that people tend to labor under a false sense of security. Fifty percent reported that their passwords were very or extremely secure, but according to the survey:

* 41 percent have shared passwords with at least one other person in the past year.

* 90 percent don’t ensure that they never use the same password on multiple accounts.
* 86 percent don’t check that they’re on a secure connection when accessing sensitive information on unfamiliar computers.
* 14 percent never change their banking password.
* 20 percent have used a significant date (such as a birthday) or a pet’s name in their passwords.
* 84 percent fail to use passwords more than ten characters long.

The findings are even more disturbing among young people. The common wisdom that young people are more tech savvy is apparently trumped by the truism that they’re more reckless; at least according to Webroot’s findings. Webroot found that among 18 to 29 year-olds:

* 12 percent have shared a password in a text message (vs. 4 percent overall).
* 30 percent logged into a site requiring a password over public Wi-Fi (vs. 21 percent overall).
* 54 percent have shared passwords with one or more people in the past year (vs. 41 percent overall).

For tips on how to how to do passwords right, read PCMag’s Password Protection: How to Create Strong Passwords <http://us.rd.yahoo.com/dailynews/zd/tc_zd/storytext/255833/38096545/SIG=12e9q9o5f/*http://www.pcmag.com/article2/0,2817,2368484,00.asp?kc=PCYH104039TX1B0000663>.
If you’re looking for an app that can do it all for you, try our Editors’ Choice password manager, LastPass 1.50 <http://us.rd.yahoo.com/dailynews/zd/tc_zd/storytext/255833/38096545/SIG=12efd1gef/*http://www.pcmag.com/article2/0,2817,2343562,00.asp?kc=PCYH104039TX1B0000663>.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.